Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1. (Original) A security deciphering apparatus comprising:

a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information;

a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and

a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M).

Claim 2. (Original) The security deciphering apparatus according to claim 1, further comprising:

a personal secret key storing unit for storing the personal secret key ({Ks}Kh) received via the public network, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

Claim 3. (Previously Presented) A data service providing apparatus for providing data requested by a communication terminal, the apparatus comprising:

a data database for storing data (M) to be provided to the communication terminal;

a hidden secret key database for storing a hidden secret key (Kh) corresponding to intrinsic identification information of a security deciphering module equipped in the communication terminal to decipher enciphered data;

a transmitting/receiving unit for performing communication with the communication terminal via a public network;

a data enciphering unit for enciphering the data (M) by using a cipher key (Ks);

a cipher key enciphering unit for enciphering the cipher key (Ks) by using the hidden secret key (Kh); and

a control unit for controlling the enciphering operations of the data and cipher key enciphering units, and controlling the transmitting/receiving unit to provide the enciphered data ({M}Ks) and a personal secret key ({Ks}Kh) via the public network.

Claim 4. (Original) The data service providing apparatus according to claim 3, wherein the security deciphering module comprises:

a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information of the security deciphering module;

a first decoding unit for decoding the personal secret key ({Ks}Kh) provided by the transmitting/receiving unit, by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and

a second decoding unit for decoding the enciphered data ({M}Ks) provided by the transmitting/receiving unit, by using the cipher key (Ks), thereby obtaining the data (M).

Claim 5. (Original) The data service providing apparatus according to claim 4, wherein the security deciphering module further comprises:

a personal secret key storing unit for storing the personal secret key ({Ks}Kh) provided by the transmitting/receiving unit, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

Claim 6. (Original) A security deciphering method comprising the steps of:

determining whether or not a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information, is received;

if it is determined that the personal secret key ({Ks}Kh) is received, then decoding the received personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks);

determining whether or not enciphered data ({M}Ks), generated by enciphering data (M) requested to be transmitted by using the cipher key (Ks), is received; and

if it is determined that the enciphered data ({M}Ks) is received, then decoding the enciphered data ({M}Ks) by using the cipher key Ks, thereby obtaining the data (M).

Claim 7. (Original) A data service providing method for providing data requested by a communication terminal, comprising the steps of:

receiving via a public network a request for transmission of data (M) from the communication terminal;

enciphering the data (M) by using a cipher key (Ks) in response to the received data transmission request, thereby generating enciphered data ({M}Ks);

enciphering, in response to the received data transmission request, the cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information assigned to a security enciphering module equipped in the communication terminal to decode the enciphered data ({M}Ks), thereby generating personal secret key ({Ks}Kh); and

transmitting the enciphered data ({M}Ks) and the personal secret key ({Ks}Kh) to the communication terminal via the public network.

Claim 8. (Original) The data service providing method according to claim 7, wherein the security enciphering module equipped in the communication terminal comprises:

a hidden secret key storing unit for storing the hidden secret key (Kh) corresponding to the intrinsic identification information assigned to the security enciphering module;

a first decoding unit for decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and

a second decoding unit for decoding the enciphered data ({M}Ks) by using the obtained cipher key (Ks), thereby obtaining the data (M).

Claim 9. (Original) The data service providing method according to claim 8, wherein the security deciphering module further comprises:

a personal secret key storing unit for storing the personal secret key ({Ks}Kh) received by the communication terminal via the public network, and outputting the stored personal secret key ({Ks}Kh) to the first decoding unit under a control of the first decoding unit; and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit, and outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit.

Claim 10. (Original) In a mobile communication terminal receiving, via a public network, enciphered data ({M}Ks) generated by enciphering data (M) by using a cipher key (Ks), a security deciphering apparatus comprising:

a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information assigned to the mobile communication terminal;

a first decoding unit for receiving a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks); and

a second decoding unit for decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M).

Claim 11. (New) A security deciphering method comprising:

providing a hidden secret key (Kh) corresponding to intrinsic identification information;

providing a cipher key (Ks);

generating a personal secret key ({Ks}Kh) by the cipher key (Ks) by using the hidden secret key (Kh); and

encoding/decoding data M using the hidden secret key (Kh), the cipher key (Ks); and the personal secret key ({Ks}Kh),

thereby achieving improved security for transmitting/receiving the data M over public networks.